

CONCEPT MAP

IOQM · NUMBER THEORY

5 TOPICS · 38 CORE IDEAS · ONE SHEET



DIVISIBILITY & PRIMES

61

DIVISIBILITY

For integers $a \neq 0$ and b , we say a **divides** b , written $a \mid b$, when $b = ak$ for some integer k .

KEY

$a \mid b, a \mid c \implies a \mid bx + cy$ for all integers x, y

- Transitive:** $a \mid b$ and $b \mid c$ give $a \mid c$.
- Size:** If $a \mid b$ and $b \neq 0$ then $|a| \leq |b|$. So a divisor of a non zero number is bounded, which is what makes divisor searches finite.
- Both ways:** $a \mid b$ and $b \mid a$ force $a = \pm b$.
- Every non zero integer divides 0, and ± 1 divide every integer.

If $n+1 \mid n^2+1$, then $n+1$ also divides $(n^2+1)-(n-1)(n+1)=2$, so $n+1 \in \{\pm 1, \pm 2\}$.

The combination rule is the workhorse of the whole chapter. Choose x and y so that the variable cancels, and the divisor is trapped inside a fixed number. Every “ d divides both, so d divides a constant” argument on this sheet is this rule.

62

THE DIVISION ALGORITHM

For any integer a and any integer $b > 0$ there is exactly one pair q, r with

KEY

$a = bq + r, \quad 0 \leq r < b$

- q is the quotient and r the remainder; $q = \lfloor a/b \rfloor$.
- The remainder is never negative.** $-17 = 5(-4)+3$, so -17 leaves remainder 3 on division by 5, not -2 .
- Every integer has exactly one of the b forms $bk, bk+1, \dots, bk+(b-1)$. Splitting into these forms is the cleanest proof by cases.
- If $d \mid a$ and $d \mid b$, then d also divides the remainder $r = a - bq$.

IOQM 2026, Q2: $4 \mid M$ and $4 \nmid 256$, so the remainder of M on division by 256 is a multiple of 4. It cannot be 0, since $256 \nmid M$, leaving 63 remainders.

63

DIVISIBILITY TESTS

DIVISOR	TEST ON THE NUMBER
2, 5	last digit; even, or 0 or 5
4	last two digits form a multiple of 4
8	last three digits form a multiple of 8
3, 9	digit sum is a multiple of 3, of 9
11	alternating digit sum from the units is a multiple of 11
7, 11, 13	alternating sum of three digit blocks from the right is a multiple of 7, 11, 13

- The tests are congruences in disguise: $10 \equiv 1 \pmod 9, 10 \equiv -1 \pmod{11}$, and $1000 \equiv -1 \pmod{1001}$, with $1001 = 7 \cdot 11 \cdot 13$.
- So a number and its digit sum leave the same remainder mod 9, and the alternating sum gives the remainder mod 11 up to sign.

123456: blocks $456-123=333=3^2 \cdot 37$, so it is not divisible by 7, 11 or 13.

For a composite divisor, test coprime factors. Divisibility by 12 is divisibility by 3 and by 4. Testing 2 and 6 proves nothing; 6 passes both and is not a multiple of 12.

64

PRIMES AND THE SIEVE

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

fifteen primes below 50; striking multiples of 2,3,5,7,13 enough, since $7 \cdot 7 < \sqrt{50} < 11$

- A **prime** is an integer $p > 1$ whose only positive divisors are 1 and p . The number 1 is neither prime nor composite, and 2 is the only even prime.
- Square root test:** If $n > 1$ has no prime factor $\leq \sqrt{n}$, then n is prime. To test 221 try primes up to 14, and 13 works: $221 = 13 \cdot 17$.
- Infinitely many primes (Euclid).** If $p_1, \dots, p_k$ were all of them, $p_1 p_2 \dots p_k + 1$ would have a prime factor outside the list.
- Gaps are unbounded:** $(n+1)!+2, (n+1)!+3, \dots, (n+1)!+(n+1)$ are n consecutive composites.

Worth memorising: there are 25 primes below 100, and the primes below 50 are the fifteen marked above. Recognising $91 = 7 \cdot 13, 119 = 7 \cdot 17, 143 = 11 \cdot 13$ and $221 = 13 \cdot 17$ on sight saves time in every paper.

65

FUNDAMENTAL THEOREM OF ARITHMETIC

Every integer $n > 1$ is a product of primes, and the product is unique apart from the order of the factors.

KEY

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

- Euclid's lemma:** If a prime p divides ab , then $p \mid a$ or $p \mid b$. It fails for composites: $6 \mid 4 \cdot 9$ but $6 \nmid 4$ and $6 \nmid 9$.
- n is a perfect square exactly when every exponent α_i is even, and a perfect k th power when every α_i is a multiple of k .
- $m \mid n$ exactly when each prime appears in m to a power no larger than in n .

Coprime factors of a square are squares. If a, b are positive, $\gcd(a, b) = 1$ and ab is a perfect square, then a and b are both perfect squares, because no prime is shared between them. This one line opens most Diophantine equations of the form $xy = z^2$.

66

NUMBER, SUM AND PRODUCT OF DIVISORS

For $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, a divisor chooses each exponent independently from 0 to α_i .

KEY

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$$

- $\tau(n)$ is odd if and only if n is a perfect square, since divisors pair as $d + n/d$ and only $\sqrt{n}$ pairs with itself.
- Ordered pairs (x, y) of positive integers with $xy = n$ number $\tau(n)$.
- σ and σ are multiplicative: $\tau(mn) = \tau(m)\tau(n)$ when $\gcd(m, n) = 1$.

$72 = 2^3 3^2$: $\tau = 4 \cdot 3 = 12$, $\sigma = 15 \cdot 13 = 195$, and the product of all divisors is 72^6 .

67

PRIMES OF SPECIAL FORM

- Every prime $p > 3$ has the form $6k \pm 1$, because the other residues mod 6 are divisible by 2 or 3.
- Every odd prime is $4k+1$ or $4k+3$, and the two kinds behave very differently (section 31).

KEY

$$p > 3 \text{ prime} \implies 24 \mid p^2 - 1$$

Proof: $p^2 - 1 = (p-1)(p+1)$ is a product of consecutive even numbers, one of them a multiple of 4, so 8 divides it; and 3 divides one of $p-1, p, p+1$ but not p .

IOQM 2026, Q25: $p^2 + p^2 - 2 = (p^2 + 2)(p-1)(p+1)$. For every prime $p > 3$, 8 · 3 divides $(p-1)(p+1)$ and 3 $\nmid p^2 + 2$, so 72 divides the value; $p = 5, 7$ give 636 and 3438, whose gcd is 72.

“Largest number dividing every value” has two halves. Prove that some D always divides, then show nothing larger can by taking the gcd of two small cases. Either half alone earns nothing.

68

FACTORISATION TOOLS

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \dots + b^{n-1})$$

- $a-b \mid a^n - b^n$ for every $n \geq 1$.
- $a+b \mid a^n + b^n$ for odd n , and $a-b \mid a^n - b^n$ for even n .
- Sophie Germain:** $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$.
- Difference of squares:** $n = x^2 - y^2 = (x-y)(x+y)$, and the two factors have the same parity. So n is a difference of two squares of integers (0 allowed) exactly when $n \neq 2 \pmod 4$; with both squares positive, 1 and 1 are the only further exceptions among positive n .

$n^4 - 4 = (n^2 + 2n + 2)(n^2 - 2n + 2)$, and the second factor equals 1 only at $n = 1$. So for positive n , $n^4 + 4$ is prime only when $n = 1$.

Factor before anything else. A difference of powers or a product of consecutive integers turns most “show this divides for every n ” questions into a single line.

69

GCD, LCM & LINEAR EQUATIONS

69

GCD AND LCM

- $\gcd(a, b)$ is the largest common divisor, and $\text{lcm}(a, b)$ the smallest positive common multiple.
- From the prime factorisations, the gcd takes the smaller exponent of each prime and the lcm the larger.
- Every common divisor divides the gcd, and every common multiple is a multiple of the lcm.
- Every common divisor divides the gcd, and every common multiple is a multiple of the lcm.
- $\gcd(ka, kb) = k \gcd(a, b)$ for $k > 0$.

KEY

$$\gcd(a, b) \cdot \text{lcm}(a, b) = ab \quad (a, b > 0)$$

The standard parametrisation: with $g = \gcd(a, b)$ write $a = gx, b = gy$ where $\gcd(x, y) = 1$. Then $\text{lcm}(a, b) = gxy$.

The product identity is an identity for two numbers only. For three numbers it holds only when they are pairwise coprime. For 2, 2, 2 the gcd and lcm are both 2, with product 4, while $abc = 8$.

70

THE EUCLIDEAN ALGORITHM

20 = 2 · 10 + 6, 10 = 1 · 6 + 4, 6 = 1 · 4 + 2, 4 = 2 · 2

the last square is the gcd: $\gcd(20, 12) = 2$

KEY

$$\gcd(a, b) = \gcd(b, a \bmod b) = \gcd(a - kb, b)$$

- Replace the larger number by its remainder on division by the smaller, and repeat. The last non zero remainder is the gcd.
- Geometrically, cut the largest possible squares off a rectangle; the side of the last square is the gcd.
- The remainders at least halve every two steps, so the method is fast even for large numbers.

$3(14n+3) - 2(21n+4) = 1$, so $\gcd(21n+4, 14n+3) = 1$ and $\frac{21n+4}{14n+3}$ is in lowest terms for every n .

71

BEZOUT'S IDENTITY

For integers a, b not both zero there are integers x, y with

KEY

$$ax + by = \gcd(a, b)$$

- $\gcd(a, b)$ is the smallest positive value of $ax + by$ over all integers x, y .
- a and b are coprime if and only if $ax + by = 1$ has an integer solution.
- To find x, y , run the Euclidean algorithm and substitute back from the last line.

From the ladder: $2 = 6 - 4 = 6 - (10 - 6) = 2 \cdot 6 - 10 = 2(26 - 2 \cdot 10) - 10 = 2 \cdot 26 - 5 \cdot 10$.

Bezout is the reason inverses exist. $ax \equiv 1 \pmod m$ is $ax + my = 1$, which is solvable exactly when $\gcd(a, m) = 1$ (section 17).

72

COPRIMALITY FACTS

- $\gcd(n, n+k)$ divides k . So consecutive integers are coprime, and two consecutive odd numbers are coprime.
- If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.
- If $a \mid n, b \mid n$ and $\gcd(a, b) = 1$, then $ab \mid n$. Without coprimality this fails: $4 \mid 12$ and $6 \mid 12$ but $24 \nmid 12$.
- Consecutive Fibonacci numbers are coprime, and $\gcd(F_m, F_n) = F_{\gcd(m, n)}$.

KEY

$$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m, n)} - 1 \quad (a \geq 2; m, n \geq 1)$$

To prove $72 \nmid N$, prove $8 \nmid N$ and $9 \nmid N$. N Always split a divisor into coprime prime powers. Splitting it as $6 \cdot 12$ or $2 \cdot 36$ proves nothing, because those factors share primes.

73

LINEAR DIOPHANTINE EQUATIONS

$3x + 5y = 17$ meets the grid every (5, -3): three positive solutions

$ax + by = c$ has integer solutions if and only if $g = \gcd(a, b)$ divides c . From one solution (x_0, y_0) , all of them are

KEY

$$x = x_0 + \frac{c}{g}t, \quad y = y_0 - \frac{a}{g}t, \quad t \in \mathbb{Z}$$

- Find (x_0, y_0) by inspection, or scale the Bezout pair by c/g .
- For positive solutions, write $x > 0$ and $y > 0$ as two inequalities in t and count the integers between them.

$3x + 5y = 47$; $x = 4 + 5t, y = 7 - 3t$. Positivity needs $-\frac{4}{5} < t < \frac{7}{3}$, so $t \in \{0, 1, 2\}$: three solutions (4, 7), (9, 4), (14, 1).

13 · 13 = 169 = 8 · 21 + 1, so $13^{-1} \equiv 13 \pmod{21}$. IOQM 2026, Q28 solves $13x_2 \equiv 512x_1 \pmod{21}$ with exactly this inverse.

Cancelling without the gcd is the commonest slip. $2 \cdot 3 \equiv 2 \cdot 8 \pmod{10}$, yet $3 \not\equiv 8 \pmod{10}$. The correct conclusion is $3 \equiv 8 \pmod 5$.

74

THE COIN PROBLEM

For coprime integers $a, b \geq 2$, the amounts that can be paid exactly with coins of values a and b are the numbers $ax + by$ with $x, y \geq 0$. The largest amount that cannot be paid is

KEY

$$ab - a - b$$

- Every integer greater than $ab - a - b$ can be paid.
- Exactly $\frac{(a-1)(b-1)}{2}$ positive integers cannot be paid.
- If $\gcd(a, b) = d > 1$, only multiples of d can ever be paid, so there is no largest impossible amount.

Stamps of 5 and 8: the largest impossible postage is $40 - 13 = 27$, and there are $\frac{4 \cdot 7}{2} = 14$ impossible amounts.

The number of non negative solutions of $ax + by = n$, with a, b coprime, is $\lfloor n/ab \rfloor$ or $\lfloor n/ab \rfloor + 1$, because consecutive solutions differ by b in x .

75

POWERS MODULO SMALL NUMBERS

POWER, MODULUS	POSSIBLE RESIDUES
$x^2 \pmod 3$ or 4	0, 1
$x^2 \pmod 5$	0, 1, 4
$x^2 \pmod 8$	0, 1, 4; odd squares are 1
$x^2 \pmod 9$	0, 1, 4, 7
$x^2 \pmod{16}$	0, 1, 4, 9
$x^2 \pmod 7$ or 9	0, ± 1
$x^4 \pmod{16}$	0, 1

- A sum of two squares is never $\equiv 3 \pmod 4$, and a sum of three squares is never $\equiv 7 \pmod 8$.
- A sum of two cubes is never $\equiv 3, 4, 5, 6 \pmod 9$.

Choose the modulus where the power has fewest residues. Use 4 or 8 for squares, 7 or 9 for cubes, 16 for fourth powers. Fewer residues means fewer cases and a faster contradiction.

76

FERMAT'S LITTLE THEOREM

For a prime p and any integer a not divisible by p ,

KEY

$$a^{p-1} \equiv 1 \pmod p$$

- Equivalently $a^p \equiv a \pmod p$ for every integer a , including multiples of p .
- So when $p \mid a$, the exponent of a may be reduced modulo $p-1$.

$3^{100} \pmod 7$: $100 \equiv 6 \cdot 16 + 4$, so $3^{100} \equiv 3^4 \equiv 81 \equiv 4 \pmod 7$.

The converse is false. $341 \equiv 11 \cdot 31$ is composite, yet $2^{340} \equiv 1 \pmod{341}$. Passing the Fermat test does not prove a number prime.

77

EULER'S THEOREM AND THE TOTIENT

$\varphi(n)$ counts the integers in $1, \dots, n$ that are coprime to n .

KEY

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

- $a^{p-1} \equiv 1 \pmod p$ and $\gcd(a, n) = 1$
- $\varphi(p) = p-1, \varphi(p^k) = p^k - p^{k-1}$, and $\varphi(mn) = \varphi(m)\varphi(n)$ when $\gcd(m, n) = 1$.
- $\sum_{d \mid n} \varphi(d) = n$.
- Euler's theorem is Fermat's theorem for any modulus; with $n = p$ it gives back $a^{p-1} \equiv 1$.

List negative divisor pairs too, then filter by the constraints. Forgetting the negative pairs is the usual way solutions go missing; forgetting the constraints is the usual way wrong ones get in.

78

MODULAR ARITHMETIC

78

CONGRUENCES

$a \equiv b \pmod m$ means $m \mid a-b$; equivalently, a and b leave the same remainder on division by m .

KEY

$$a \equiv b, c \equiv d \pmod m \implies a \pm c \equiv b \pm d, ac \equiv bd, a^k \equiv b^k$$

- Reduce as early as possible: $2026 \equiv 1 \pmod 5$, so $2026^{100} \equiv 1 \pmod 5$.
- For a polynomial P with integer coefficients, $a \equiv b$ gives $P(a) \equiv P(b) \pmod m$. Equivalently $a-b \mid P(a) - P(b)$.

Exponents do not reduce mod m . $2^{10} \equiv 1024 \equiv 2 \pmod 7$, while $2^{10 \bmod 7} \equiv 2^3 \equiv 1$. When a is coprime to m , exponents reduce modulo the order (section 23), here $3 \cdot 2^3 \equiv 2^4$.

79

INVERSES AND CANCELLATION

$$ac \equiv bc \pmod m \implies a \equiv b \pmod{\frac{m}{\gcd(m, c)}}$$

- So a common factor cancels freely only when it is coprime to the modulus.
- a has an inverse mod m , a number a^{-1} with $aa^{-1} \equiv 1$, exactly when $\gcd(a, m) = 1$, and it is unique mod m .
- Modulo a prime, every non zero residue has an inverse, so division by anything non zero is allowed.

13 · 13 = 169 = 8 · 21 + 1, so $13^{-1} \equiv 13 \pmod{21}$. IOQM 2026, Q28 solves $13x_2 \equiv 512x_1 \pmod{21}$ with exactly this inverse.

Cancelling without the gcd is the commonest slip. $2 \cdot 3 \equiv 2 \cdot 8 \pmod{10}$, yet $3 \not\equiv 8 \pmod{10}$. The correct conclusion is $3 \equiv 8 \pmod 5$.

80

CHINESE REMAINDER THEOREM

each of 0, ..., 11 fills one cell; $x \equiv 2 \pmod 3, x \equiv 3 \pmod 4$ gives $x \equiv 11 \pmod{12}$

$$x \equiv a_1 \pmod{m_1}, \dots, x \equiv a_k \pmod{m_k}$$
$$\gcd(m_1, m_2) = 1 \implies \text{one } x \pmod{m_1 m_2}$$

If $m_1, \dots, m_k$ are pairwise coprime, the system $x \equiv a_i \pmod{m_i}$ has exactly one solution modulo $m_1 m_2 \dots m_k$.

- Solve by stepping: list the numbers satisfying the larger modulus and take the first that fits the others.
- Use it in reverse: to find N mod 100, find N mod 4 and N mod 25 separately and glue them.
- For moduli that are not coprime, the system is solvable iff $a_i \equiv a_j \pmod{\gcd(m_i, m_j)}$, and then the solution is unique modulo the lcm.

$x \equiv 2 \pmod 3, x \equiv 3 \pmod 5, x \equiv 7 \pmod 7$ gives $x \equiv 23 \pmod{105}$.

81

PERFECT SQUARES

$$n^2 < N < (n+1)^2 \implies N \text{ is not a perfect square}$$

- Squeeze the expression between two consecutive squares; nothing in between is a square.
- A square ends in 0, 1, 4, 5, 6 or 9, and a square ending in 5 ends in 25.
- The number of squares in $1, \dots, N$ is $\lfloor \sqrt{N} \rfloor$.
- $n(n+1)(n+2)(n+3) + 1 = (n^2 + 3n + 1)^2$.

For $n \geq 1, n^2 < n^2 + n + 1 < (n+1)^2$, so $n^2 + n + 1$ is never a perfect square.

The squeeze is the most used tool for “find all n for which this is a square”. Bound the expression between $(n+a)^2$ and $(n+a+1)^2$ for large n , then check the few small n left over by hand.

82

SUMS OF TWO SQUARES

- Fermat: an odd prime p is a sum of two squares if and only if $p \equiv 1 \pmod 4$; and $2 = 1^2 + 1^2$.
- A positive integer is a sum of two squares if and only if every prime $\equiv 3 \pmod 4$ divides it to an even power.
- Since squares are 0 or 1 mod 4, a number $\equiv 3 \pmod 4$ is never a sum of two squares.

KEY

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

IOQM 2026, Q10: of 0, 1, ..., 20, exactly 13 are sums of two squares. The failures are 3, 7, 11, 15, 19 and 6, 12, 14, each with a prime $\equiv 3 \pmod 4$ to an odd power.

The product identity gives the “ $\frac{1}{4}$ ” half: products of 2, primes $\equiv 1 \pmod 4$ and squares v^2 are sums of two squares. The “only $\frac{1}{4}$ ” half uses a separate fact: a prime $q \equiv 3 \pmod 4$ dividing $x^2 + y^2$ divides both x and y .

83

LAST DIGITS AND LAST TWO DIGITS

LAST DIGIT OF a	LAST DIGITS OF $a, a^2, a^3, \dots$
2	2, 4, 8, 6, period 4
3	3, 9, 7, 1, period 4
7	7, 9, 3, 1, period 4
8	8, 4, 2, 6, period 4
4, 9	4, 6 and 9, 1, period 2
0, 1, 5, 6	constant

- For $n \geq 1$, reduce n modulo 4; a remainder of 0 means the fourth entry of the cycle, not the first.
- For the last two digits, work mod 4 and mod 25. When $\gcd(a, 10) = 1, a^{20} \equiv 1 \pmod{100}$.

The a^{20} shortcut needs a coprime to 10. For 2^n with $n \geq 2$, use $2^n \equiv 0 \pmod 4$ and $2^{20} \equiv 1 \pmod{25}$ separately, then glue by section 24.

84

DIGITS, SQUARES & EQUATIONS

84

LEGENDRE'S FORMULA

Every primitive triple, one with $\gcd(x, y, z) = 1$, has the form below, with the legs possibly swapped, where $m > n \geq 1, \gcd(m, n) = 1$ and $m - n$ odd; every triple is a multiple of a primitive one.

KEY

$$(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$$

- In a primitive triple the hypotenuse is odd and exactly one leg is even.
- In every triple one leg is a multiple of 3, one leg a multiple of 4, and one side a multiple of 5. So the product of the legs is a multiple of 12, and of all three sides a multiple of 60.

$(m, n) = (3, 2)$ gives (5, 12, 13); (4, 1) gives (15, 8, 17); (5, 2) gives (21, 20, 29).

85

EULER'S THEOREM AND THE TOTIENT

$\varphi(n)$ counts the integers in $1, \dots, n$ that are coprime to n .

KEY

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

- $a^{p-1} \equiv 1 \pmod p$ and $\gcd(a, n) = 1$
- $\varphi(p) = p-1, \varphi(p^k) = p^k - p^{k-1}$, and $\varphi(mn) = \varphi(m)\varphi(n)$ when $\gcd(m, n) = 1$.
- $\sum_{d \mid n} \varphi(d) = n$.
- Euler's theorem is Fermat's theorem for any modulus; with $n = p$ it gives back $a^{p-1} \equiv 1$.

$\varphi(100) = 100 \cdot \frac{1}{2} \cdot \frac{1}{5} = 40$. But $7^4 = 2401 \equiv 1 \pmod{100}$ already: $\varphi(n)$ is a period, not always the shortest.

86

WILSON'S THEOREM

86

WILSON'S THEOREM

KEY

$$(n-1)! \equiv -1 \pmod n$$

- Why: modulo p , the residues $2, \dots, p-2$ pair off with their inverses, which are distinct from themselves, so each pair contributes 1. Only 1 and $p-1$ are their own inverses, leaving $1 \cdot (p-1) \equiv -1$.
- The converse holds too: for composite $n > 4, (n-1)! \equiv 0 \pmod n$, and for $n = 4$ it is 2; so for $n \geq 2$ the congruence characterises the primes.

for $n \geq 2$: n prime $\iff (n-1)! \equiv -1 \pmod n$

16! $\equiv -1 \pmod{17}$ and $16! \equiv 16 \cdot 15! \equiv -15! \pmod{17}$, so $15! \equiv 1 \pmod{17}$.

87

ORDER, AND CYCLES OF POWERS

For $\gcd(a, m) = 1$, the order ord $_m(a)$ is the least $d \geq 1$ with $a^d \equiv 1 \pmod m$. The powers of a then repeat with period d .

KEY

$$a^{n^2} \equiv 1 \pmod m \iff \text{ord}_m(a) \mid n$$

- So the order divides $\varphi(m)$, and divides $p-1$ for a prime p . To find it, test only the divisors of $\varphi(m)$.
- If $d \mid n$ then $a^d \equiv 1 \pmod m$.
- For a prime $p \neq 2$, the decimal period of $1/p$ is ord $_p(10)$; $10^8 \equiv -1 \pmod{13}$, so $1/13$